The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
11/3/2020

SUBJECT:
Multiple Vulnerabilities in Adobe Acrobat and Adobe Reader Could Allow for Arbitrary Code Execution (APSB20-67)

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe Acrobat and Adobe Reader, the most severe of which could allow for arbitrary code execution. Adobe Acrobat is a family of software developed by Adobe Inc. to view, create, manipulate, print, and manage files in PDF format. Adobe Reader is the free version within the Adobe Acrobat family of software. Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Acrobat DC (Continuous track) for Windows & macOS version 2020.012.20048 and earlier versions
- Acrobat Reader DC (Continuous track) for Windows & macOS version 2020.012.20048 and earlier versions
- Acrobat 2020 (Classic 2020) for Windows & macOS version 2020.001.30005 and earlier versions
- Acrobat Reader 2020 (Classic 2020) for Windows & macOS version 2020.001.30005 and earlier versions
- Acrobat 2017 (Classic 2017 track) for Windows & macOS version 2017.011.30175 and earlier versions
- Acrobat Reader 2017 (Classic 2017 track) for Windows & macOS version 2017.011.30175 and earlier versions

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Adobe Acrobat and Adobe Reader, the most severe of which could allow for arbitrary code execution. Details of the vulnerabilities are as follows:

- A Heap-based buffer overflow vulnerabilities that could allow for arbitrary code execution. (CVE-2020-24435)
- A Improper access control vulnerability that could allow for local privilege escalation. (CVE-2020-24433)
- A Improper input validation vulnerability that could allow for arbitrary JavaScript execution. (CVE-2020-24432)
- A Signature validation bypass vulnerability that could allow for minimal (defense-in-depth fix). (CVE-2020-24439)
- A Signature verification bypass vulnerability that could allow for local privilege escalation. (CVE-2020-24429)
- A Improper input validation vulnerability that could allow for information disclosure. (CVE-2020-24427)
- A Security feature bypass vulnerability that could allow for Dynamic library injection. (CVE-2020-24431)
- An Out-of-bounds write vulnerability that could allow for arbitrary code execution. (CVE-2020-24436)
- Multiple Out-of-bounds read vulnerabilities that could allow for information disclosure. (CVE-2020-24426, CVE-2020-24434)
- A Race Condition vulnerability that could allow for local privilege escalation. (CVE-2020-24428)
- Multiple Use-after-free vulnerabilities that could allow for arbitrary code execution. (CVE-2020-24430, CVE-2020-24437)
- A Use-after-free vulnerability that could allow for information disclosure. (CVE-2020-24438)

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.

- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
https://helpx.adobe.com/security/products/acrobat/apsb20-67.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24435
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24433
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24432
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24439
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24429
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24427
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24431
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24436
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24426
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24434
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24428
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24430
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24437
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24438